JOURNAL OF NUMBER THEORY 1, 116–120 (1969)

On the Factorization of Polynomials

H. KEMPFERT*

Department of Mathematics, The Ohio State University, Columbus, Ohio 43210

Communicated by H. Zassenhaus

Received May 15, 1968

Given a polynomial $f(x)$ with rational integral coefficients, find the factorization of $f(x)$ into irreducible factors for a given characteristic, a natural prime p or zero. In the latter case we use the factorization of $f(x)$ for a special natural prime p.

I. THE FACTORIZATION OF POLYNOMIALS mod p

The problem of complete factorization of a polynomial $f(x)$ is equivalent with the task to find a proper factor of $f(x)$ or to recognize $f(x)$ to be an irreducible polynomial itself.

Step 1. Let $f(x)$ be a polynomial of degree n, $n > 1$, and leading coefficient 1. Calculate the derivative $f'(x)$ of $f(x)$. If $f'(x) = 0$, then $f(x)$ is the pth power of a proper factor. If $f(x)$ is inseparable and $f'(x) \neq 0$, then $(f(x), f'(x))$ is a proper factor of $f(x)$.

Step 2. Assume $f(x)$ to be separable. Compute

$$(f(x), x^{p^m-1}-1)$$

for ascending m. $f(x)$ is irreducible if $f(x)$ does not factor for $m = 1, \ldots, \left[\frac{n}{2}\right]$.

Remark. $(f(x), x^{p^m-1}-1) = (f(x), x^{p^m}-x)$ provided $x \nmid f(x)$. We need x^{p^m} only mod $f(x)$. According to E. R. Berlekamp [1] one can calculate an $n \times n$-matrix Q which transforms the coefficient vector $(g_0, \ldots, g_{n-1})$ of any polynomial $g(x)$ of degree less than n into the vector $(h_0, \ldots, h_{n-1})$

* Author's current address: Zuse KG, 643 Bad Hersfeld, Grosse Industriestr. 19 u. 21, West Germany.

representing the polynomial $h(x)$ which satisfies the relation

$$h(x) \equiv g(x)^p \bmod (f(x), p).$$

Step 3. Assume

$$f(x) = (f(x), x^{p^m-1}-1), \tag{1}$$

$$f(x) = \prod_{i=1}^{r} \varphi_i(x), \qquad [\varphi_i(x)] = m, \qquad \varphi_i(x) \text{ irreducible.}$$

Reduce $x^k \bmod f(x)$, $k = \sum_{j=0}^{n-1} p^j$, by a special algorithm. If

$$x^k \equiv a \bmod (f(x), p), \qquad a \in \mathbf{Z},$$

then go to step 5 else to step 4. The probability that $f(x)$ divides mod p one factor of (2) is (neglecting any structure that might be involved) $(p-1)^{1-r}$, this is the probability for the application of step 5. Step 4 gives always at least one proper factor of $f(x)$.

Step 4. Assume (1), $r \geqq 2$, $p \geqq 3$, and the existence of at least two constants a_1, a_2 with the property

$$(x^k - a_i, f(x)) \neq 1, f(x), \qquad i = 1, 2.$$

Decompose the product

$$x^{p^m-1}-1 = \prod_{a=1}^{p-1} (x^k - a) \tag{2}$$

into suitable groups of factors and calculate the *gcd*'s with $f(x)$.

Let $s|(p-1)$. Then we have

$$x^{p^m-1}-1 = \prod_{t=1}^{(p-1)/s} (x^{ks} - g^{st})$$

$$= \prod_{t=1}^{p-1} (x^k - g^t), \qquad g \text{ a primitive root mod } p, \tag{3}$$

because $x^{p^m-1}-1$ is a separable polynomial and any factor $x^k - x^t$ divides $x^{ks} - g^{st_1}$, provided $t \equiv t_1 \bmod ((p-1)/s)$. Actually we need only the system of the sth power residues mod p. If one has to factor many polynomials with respect to the same prime p, it is convenient to calculate a primitive root g and prepare a list of power residues for all proper divisors s of $p-1$ in advance.

In the special case $s = (p-1)/2$ the factorization

$$x^{p^m-1}-1 = (x^{(p^m-1)/2}-1)(x^{(p^m-1)/2}+1)$$

is always possible. The probability that we obtain already a factorization of $f(x)$ just by considering $s = (p-1)/2$ is $(1-2^{1-r})$.

Step 5. Assume $f(x) = (f(x), x^k - a)$. If $x^k - a$ can be factored easily into suitable factors, do it and calculate the *gcd*'s with $f(x)$. Maybe the number a is an hth power residue mod p, h a divisor of k. Otherwise try successively to factor t different polynomials

$$g_i(x) = f(x + b_i), \qquad i = 1, \ldots, t,$$

(go to step 3), and make the back transformation for the factors of $g_i(x)$ in the case of success. The number t should be small, depend only on p, and be chosen conveniently as practice suggests, perhaps one will choose only $t = 1, 2$.

If this method fails to factor $f(x)$ (or a factor of the original polynomial) after t trials, use a straightforward method for the factorization, e.g. the Berlekamp method [1], which is efficient for very small primes.

II. The Factorization of Polynomials for Characteristic 0

Step 1. Let $f(x)$ be a polynomial of degree n, $n > 1$. If $f(x)$ is an inseparable polynomial, $(f(x), f'(x))$ is a proper factor of $f(x)$.

Step 2. Assume $f(x)$ to be separable with respect to characteristic 0 and leading coefficient 1. From $f(x) = g(x)h(x)$ follows $f(x) \equiv g(x)h(x) \bmod p$, p any prime.

Factor $f(x) \bmod p$, p a suitable prime. We choose the prime p in such a manner that the factorization mod p of an average polynomial $f(x)$ does not take too much time while the prime p is as big as possible. Using the above described method, $p = 31, 211, 311$ ($p-1 = 2 \cdot 3 \cdot 5, 2 \cdot 3 \cdot 5 \cdot 7, 2 \cdot 3 \cdot 5 \cdot 11$), seem to be suitable primes.

If $f(x)$ is irreducible mod p, we are done, else go to step 3.

Step 3. Use the factorization of $f(x) \bmod p$ and make a list of all decompositions of $f(x)$ into two factors. Calculate upper bounds $c_1, \ldots, c_{n-1}$ for the absolute values of the first $n-1$ elementary symmetric functions of any subset of the roots of $f(x)$. Try to extend the decompositions of $f(x) \bmod p$ to decompositions for characteristic 0. The details for one decomposition are shown in the next step.

Step 4. Let

$$f(x) \equiv a_1(x)\, b_1(x) \bmod p,$$

without loss of generality we assume $[a_1(x)] \leqq [b_1(x)]$. Test whether there exist polynomials $a(x)$, $b(x)$ with the properties

$$f(x) = a(x)\, b(x), \qquad a(x) \equiv a_1(x) \bmod p, \qquad b(x) \equiv b_1(x) \bmod p.$$

If possible, we construct a sequence of polynomials $a_i(x)$, $b_i(x)$ with the following properties:

$$a_i(x) = x^r + \sum_{j=0}^{r-1} a_{ij} x^j, \qquad |a_{ij}| \leqq \left[\frac{p^i}{2}\right], c_{r-j}, \tag{4}$$

$$b_i(x) = x^t + \sum_{j=0}^{t-1} b_{ij} x^j, \qquad |b_{ij}| \leqq \left[\frac{p^i}{2}\right], c_{t-j}, \tag{5}$$

$$f(x) \equiv a_i(x)\, b_i(x) \bmod p^i, \tag{6}$$

$$a_i(x) \equiv a_1(x) \bmod p, \qquad b_i(x) \equiv b_1(x) \bmod p. \tag{7}$$

If this construction breaks down, then the test is negative and we take the next pair of factors of the list prepared by step 3. If this test is positive we apply step 3 on the factors of $a(x)$, $b(x)$ provided they are not irreducible mod p.

The construction of the sequence $a_i(x)$, $b_i(x)$ goes as follows: Let $c(x)$ be the greatest common divisor of $a_1(x)$, $b_1(x) \bmod p$, $\bar{a}_1(x)$, $\bar{b}_1(x)$ defined by

$$\bar{a}_1(x) \equiv a_1(x)/c(x) \bmod p,$$

$$\bar{b}_1(x) \equiv b_1(x)/c(x) \bmod p,$$

$u(x)$, $v(x)$ a solution of

$$c(x) \equiv a_1(x)u(x) + b_1(x)v(x) \bmod p, \tag{8}$$

$$[u(x)] < [\bar{b}_1(x)], \qquad |u_j| \leqq \frac{p}{2}, \qquad j = 0, \ldots, \bar{t}-1,$$

$$[v(x)] < [\bar{a}_1(x)], \qquad |v_j| \leqq \frac{p}{2}, \qquad j = 0, \ldots, \bar{r}-1,$$

and

$$g_i(x) \equiv (f(x) - a_i(x)\, b_i(x))/p^i, \qquad |g_{ij}| \leqq p/2, \qquad j = 0, \ldots, n-1.$$

In order to solve the congruence (6) for $i+1$ we have to be able to solve the following congruence

$$g_i(x) \equiv a_1(x)\, z_i(x) + b_1(x)\, w(x) \bmod p \tag{9}$$

for the differences

$$w_i(x) = (a_{i+1}(x) - a_i(x))/p^i$$

and

$$z_i(x) = (b_{i+1}(x) - b_i(x))/p^i.$$

If $c(x) \nmid g_i(x) \bmod p$, then the congruence (9) is not solvable and the test is negative.

If $f(x)-a_i(x)b_i(x) = 0$ the test is positive. If $\bar{g}_i(x) = g_i(x)/c(x) \equiv 0 \bmod p$, we just replace i by $i+1$ and continue the process. If $\bar{g}(x) \not\equiv 0 \bmod p$ we go ahead to solve the congruence (9). From (8) and (9) we get the following congruences:

$$\bar{g}_i(x) \equiv \bar{g}_i(x)(\bar{a}_1(x)u(x)+\bar{b}_1(x)v(x)) \bmod p,$$
$$z_i(x) \equiv \bar{g}_i(x)u(x) \bmod (p, \bar{b}_1(x)),$$
$$w_i(x) \equiv \bar{g}_i(x)v(x) \bmod (p, \bar{a}_1(x)).$$

We put now

$$a_{i+1,j} = a_{ij}+p^i w_{ij}, \qquad j = 0,\ldots,r-1,$$
$$b_{i+1,j} = b_{ij}+p^i z_{ij}, \qquad j = 0,\ldots,t-1,$$

and reduce the coefficients of $a_{i+1}(x)$, $b_{i+1}(x) \bmod p^{i+1}$ to its lowest absolute terms (if p is odd they are automatically reduced).

Now we check the conditions (4) and (5), if they are satisfied we replace i by $i+1$ and continue the process, otherwise the test is negative.

Remark. I do not consider this solution as the final answer to the proposed problem. But I do hope that this paper will give some stimulation in order to find a more satisfactory solution. Part I is unsatisfactory, because in some instances it is necessary to use a straightforward method. For large primes this should occur only very rarely. The number of trials in step 4 of part II might become large if the constants $c_1,\ldots,c_{n-1}$ are very large. In order to improve the method one may use a larger prime of similar type and normalize the given polynomial by a linear transformation $y = x+a$ such that $|f_{n-1}| \leqq n/2$, which means that the origin of the complex plane is close to the centroid of the roots of $f(x)$. A similar p-adic method was used by H. Zassenhaus [4], raising the exponent of the p-powers in each step by a factor 2.

ACKNOWLEDGMENT

For suggestions and critical discussions I am grateful to H. Zassenhaus and H. G. Zimmer.

REFERENCES

1. BERLEKAMP, E. R. On the factorization of polynomials over finite fields. Bell Telephone Laboratories, Inc., Murray Hill, N.J. (1967).
2. LLOYD, D. B., and REMMERS, H. Polynomial factor tables over finite fields. *Math. Alogs.* **2** (1967), 85–99.
3. ZASSENHAUS, H. Über die Fundamentalkonstruktionen der endlichen Körpertheorie. To be published.
4. ZASSENHAUS, H. The Hensel factorization method. To be published.